Neverquest Trojan: Built to Steal from Hundreds of Banks

By Serge Malenkovich

Published: 2013-11-29 · Archived: 2026-04-06 02:52:55 UTC

Neverquest is a new banking trojan that spreads itself via social media, email and file transfer protocols. It possesses the capacity to recognize hundreds of online banking and other financial sites. When an infected user attempts to login to one of the sites the trojan reacts by activating itself and pilfering its victim's credentials.

Neverquest then relays the stolen credentials back to a command and control server. Once there, the attackers can use the credentials to log into affected accounts via virtual network computing (VNC). VNC is essentially a shared desktop system, so the criminals basically use the victim's computer to log into the victim's online bank and perform the theft. It makes it quite impossible for the bank to distinguish legitimate users from criminals.

Kaspersky Lab announced earlier this week that the trojan has infected thousands of user-machines but – as malware expert Sergey Golovanov explains – it has the potential to do much more damage throughout the holiday season because of its efficient and versatile self-replication features. In fact, back in 2009, the Bredolab malware used the same methods of distribution that Neverquest is currently using. Bredolab would eventually become the third most widely distributed piece of malware on the Internet.

"When a user on an infected machine visits one of the sites on the list, the malware controls the browser's connection with the server," Golovanov explained in an analysis on Securelist. "Malicious users can obtain usernames and passwords entered by the user, and modify webpage content. All of the data entered by the user will be entered onto the modified webpage and transmitted to malicious users."

Once the attacker has control of a victim's account, he can empty it completely into an account under his control. In many cases, however, Golovanov notes that the attackers are moving the stolen money through a series of victim accounts. In this way, they dump money from one victim's account into another and repeat this process several times before directly obtaining the money themselves in order to make their activities difficult to trace.

Attackers dump money from one victim's account into another and repeat this process several times before directly obtaining the money themselves in order to make their activities difficult to trace.

Neverquest is for sale on at least one underground forum. It only seems to affect users browsing with Internet Explorer and Mozilla Firefox, but Neverquest's creators boast that it can be modified to attack "any bank in any country."

The malware also contains a feature that searches for specific banking-related keywords while the infected user surfs the web. If a user visits a site that includes these keywords, the trojan activates itself and begins intercepting user communications and sending them back to the attackers. If the site the victim is visiting ends up being a bank, the attackers add this new site to the list of sites that automatically trigger Neverquest. This update is then sent along through Neverquest's command and control infrastructure to all other infected machines.

Fidelity.com, the website of one of the world's largest mutual fund investment firms, appears to be one of the trojan's top targets according to the report.

"Its website offers clients a long list of ways to manage their finances online," Golovanov wrote on Securelist. "This gives malicious users the chance to not only transfer cash funds to their own accounts, but also to play the stock market, using the accounts and the money of Neverquest victims."

Neverquest is also designed to start harvesting data when an infected user visits any number of sites not related to finance, including Google, Yahoo, Amazon AWS, Facebook, Twitter, Skype and many more.

"The weeks prior to the Christmas and New Year holidays are traditionally a period of high malicious user activity," Golovanov wrote. "As early as November, Kaspersky Lab noted instances where posts were made in hacker forums about buying and selling databases to access bank accounts and other documents used to open and manage the accounts to which stolen funds are sent. We can expect to see mass Neverquest attacks towards the end of the year, which could ultimately lead to more users becoming the victims of online cash theft."

He continues:

"Protection against threats such as Neverquest requires more than just standard antivirus; users need a dedicated solution that secures transactions. In particular, the solution must be able to control a running browser process and prevent any manipulation by other applications." Luckily, Kaspersky Lab has such technology called Safe Money. As a part of Kaspersky Internet Security and Kaspersky PURE, it protects user's interactiona with financial sites, paying specific attention to the security of the encrypted connection and the absence of third-party control over web browsers.
